How Many Quantum Correlations Are Not Local?*

Carlos E. González-Guillén[1], C. Hugo Jiménez[2], Carlos Palazuelos[3], and Ignacio Villanueva[4]

1 **Departamento de Matemáticas del Área Industrial, E.T.S.I. Industriales, UPM, 28006 Madrid, Spain;**
Department of Mathematics and Statistics, University of Ottawa, K1N6N5 Ottawa, ON – Canada
carlos.gguillen@upm.es

2 **Departamento de Matemática, Universidad Federal de Minas Gerais, 30161970 Belo Horizonte, MG – Brasil**
hugo@mat.ufmg.br

3 **Departamento de Análisis Matemático, UCM, 28040 Madrid, Spain;**
Instituto de Ciencias Matemáticas (ICMAT), 28049 Madrid, Spain
carlospalazuelos@ucm.es

4 **Departamento de Análisis Matemático and IMI, UCM, 28040 Madrid, Spain**
ignaciov@ucm.es

Abstract

We study how generic is the property of nonlocality among the set of quantum correlations for bipartite dichotomic measurements. To do so, we consider the characterization of these quantum correlations as those of the form $\gamma = (\langle u_i, v_j \rangle)_{i,j=1}^n$, where the vectors u_i and v_j are in the unit sphere of a real Hilbert space. The important parameters in this description are the number of vectors n and the dimension of the Hilbert space m. Thus, it is natural to study the probability of a quantum correlation being nonlocal as a function of $\alpha = \frac{m}{n}$, where the previous vectors are independent and uniformly distributed in the unit sphere of $\mathbb{R}^m$. In this situation, our main result shows the existence of two completely different regimes: There exists an $\alpha_0 > 0$ such that if $\alpha \leq \alpha_0$, then γ is nonlocal with probability tending to 1 as $n \to \infty$. On the other hand, if $\alpha \geq 2$ then γ is local with probability tending to 1 as $n \to \infty$.

1998 ACM Subject Classification H.1.1 Systems and Information Theory

Keywords and phrases nonlocality, quantum correlations, Bell inequalities, random matrices

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.39

1 Introduction

Local measurements performed by two spatially separated observers on entangled bipartite quantum states can lead to correlations which cannot be explained by Local Hidden Variable Models (LHVM) [7]. This phenomenon, known as *quantum nonlocality*, is one of the most relevant features of quantum mechanics. In fact, though initially discovered in the context of foundations of quantum mechanics, during the last decade quantum nonlocality has become a crucial resource in many applications; some of them are quantum cryptography ([1], [2], [17]), communication complexity ([8]) and random number generators ([15], [18]).

* This work was partially supported by Spanish projects MTM2011-26912, MTM2012-30748, MTM2014-54240-P, QUITEMAD+ and "Ramón y Cajal" program, Mexico's National Council for Science and Technology postdoctoral grant 180486 and Canadian grants ER-09-06-172 and NSERC discovery grant RGPIN/341303-2010

Both from the fundamental and the resource point of view, we are interested in quantifying quantum nonlocality. That is, somehow measuring "how much" nonlocality is available in a given situation. The most used tool to quantify nonlocality is the violation of a Bell inequality, and by now there is an abundance of results quantifying the maximum possible violation in a large variety of contexts.

Another important point of view when quantifying a given resource is not only to look at the extremal cases (that is, the maximal violations) but at the "typical" cases. That is, we would like to know not only how much quantum nonlocality we have in certain extremal situations, but also how likely it is to find quantum nonlocality in a random situation.

This second problem is, so far, much less understood than the first. One of the first steps in this direction is [3]. In there, the authors prove that for almost every randomly chosen (in a precisely defined way) XOR game, its quantum value will be strictly bigger than its local value. Put in another way, the result says that almost every such game will serve as a witness that certain quantum correlation is not local.

In this work we study the "dual problem": if we consider a random quantum correlation, how likely is it that it is nonlocal? We state next the definitions needed for a precise formulation of our question.

We will work in the context where two spatially separated observers, Alice and Bob, perform dichotomic (two-outcome) measurements on a bipartite quantum state ρ, each on their part of the system, and consider the correlations between their answers.

According to the postulates of quantum mechanics, a two-outcome measurement for Alice (resp. Bob) is given by $\{A^+, A^-\}$ (resp. $\{B^+, B^-\}$), where $A^\pm$ (resp. $B^\pm$) are projectors acting on a Hilbert space and summing to the identity. We define the observable corresponding to Alice's (Bob's) measurement as $A = A^+ - A^-$ ($B = B^+ - B^-$). The joint correlation of Alice's and Bob's measurement results, denoted by a and b respectively, is $\langle ab\rangle = tr(A \otimes B\rho)$. Motivated by this, we say that $\gamma = (\gamma_{i,j})_{i,j=1}^n$ is a *quantum correlation matrix* and denote by $\gamma \in \mathcal{Q}$, if there exist a density matrix ρ acting on a tensor product of Hilbert spaces $H_1 \otimes H_2$ and two families of contractive self-adjoint operators $\{A_i\}_{i=1}^n$, $\{B_i\}_{i=1}^n$ acting on H_1 and H_2 respectively such that

$$\gamma_{i,j} = tr(A_i \otimes B_j \rho) \text{ for every } i,j = 1, \cdots, n. \tag{1}$$

That is, γ is a matrix whose entries are the correlations obtained in an Alice-Bob scenario where each of the observers can choose among n different possible dichotomic measurements. On the other hand, we say that $\gamma = (\gamma_{i,j})_{i,j=1}^n$ is a *local correlation matrix* if it belongs to the convex hull of deterministic correlations. That is,

$$\mathcal{L} = conv\Big\{(\alpha_i\beta_j)_{i,j=1}^n, \alpha_i = \pm 1, \beta_j = \pm 1,\ i,j = 1, \cdots, n\Big\}. \tag{2}$$

Local correlation matrices are precisely those whose entries are the correlations obtained in an Alice-Bob scenario when the measurement procedure can be explained by means of a LHVM. It is well known ([16]) that $\mathcal{L}$ and $\mathcal{Q}$ are convex sets satisfying

$$\mathcal{L} \subsetneq \mathcal{Q} \subsetneq K_G\mathcal{L},$$

where $1.67696... \leq K_G \leq 1.78221...$ is the so called *Grothendieck's constant*. Indeed, the first strict inclusion exactly means that there exist quantum correlations which cannot be explained by means of a LHVM (what we have called quantum nonlocality above) while the second inclusion is a consequence of Grothendieck's inequality (see Theorem 5 below) and a result proved by Tsirelson ([16]) which states that $\gamma = (\gamma_{i,j})_{i,j=1}^n$ is a quantum correlation

matrix if and only if there exist a real Hilbert space H and unit vectors $u_1, \cdots, u_n, v_1, \cdots, v_n$ in H such that

$$\gamma_{i,j} = \langle u_i, v_j \rangle \quad \text{for every } i, j = 1, \cdots, n. \tag{3}$$

We want to choose now a probability distribution on the set of quantum correlations. It is not obvious how to do so. One may try to use expression (1) as a guide, and choose a probability distribution on the set of states ρ and on the set of families of self-adjoint and contractive operators $A_1, \cdots, A_n, B_1, \cdots, B_n$. But it is not obvious how to choose a natural candidate for this second probability distribution.

Instead of that, we look at the equivalent reformulation (3) of a quantum correlation. In this (more mathematical, less physical) expression, there is indeed a natural probability distribution: we can consider the vectors $u_1, \cdots, u_n, v_1, \cdots, v_n$ independently uniformly distributed on the unit sphere of $\mathbb{R}^m$. It is well known that this is exactly the same as considering independent normalized m-dimensional gaussian vectors. Due to the Central Limit Theorem, this last fact makes it likely that different physically realistic models yield probability distributions related to this one.

Our results will depend on the relation between the dimension m and the number of questions n. It is simple to see that if one fixes any finite m, the probability that a quantum correlation matrix γ sampled according to the previous procedure is nonlocal tends to one as n tends to infinity. It is also simple to see that if n is fixed and m tends to infinity, then the probability that γ is not local converges to 0. See [12] for details.

Remarkably, our main result says that in the "constant ratio regime", where the ratio $\alpha = \frac{m}{n}$ remains constant as n grows, both extreme cases are possible: γ will be almost surely local for α big enough, whereas γ will be almost surely non local for α small enough.

Specifically, the main result of our work can be condensed as:

▶ **Theorem 1.** *Let n and m be two natural numbers and $\alpha = \frac{m}{n}$. Let us consider $2n$ random vectors $u_1, \cdots, u_n, v_1, \cdots, v_n$ independent and uniformly distributed on the unit sphere of $\mathbb{R}^m$ and let us denote by $\gamma = (\langle u_i, v_j \rangle)_{i,j=1}^n$ the corresponding quantum correlation matrix.*

(a) *If $\alpha \leq \alpha_0 \approx 0.004$ then γ is nonlocal with probability tending to one as n tends to infinity.*

(b) *If $\alpha \geq 2$, then γ is local with probability tending to one as n tends to infinity.*

This result shows clearly the need of studying the problem as a function of the parameter $\alpha = \frac{m}{n}$. One possible way to think of this problem is the following: say that we want to sample our vectors on a space of large dimension m. In that case, how many vectors $u_1, \cdots, u_n, v_1, \cdots, v_n$ will we need to sample in order to have nonlocality with high probability? Our results show that $n = \frac{m}{2}$ will be too few vectors, whereas $n = \frac{m}{\alpha_0}$ will be enough.

Curiously enough, we will see below that if one considers normalized vectors whose entries are independent Bernoulli variables, the probability of obtaining a nonlocal correlation matrix is zero, since all of them will be local. This means that, in contrast to many other contexts in random matrix theory, considering gaussian and Bernouilli random variables in our problem leads to completely different conclusions.

The probability distribution we consider on the random correlations arises from a mostly mathematical point of view. Despite that, in Section 5 we show a physical model which yields that same probability distribution.

The paper is organized as follows: In Section 2 we introduce some basic results that will illustrate the technics used along the whole paper. The main theorem is divided in

two parts, as each of them requires quite different techniques. The precise statement and a sketch of the proof of part a) of the theorem, based on results from random matrix theory, is given in Section 3, while Section 4 states precisely part b) and sketches its proof. Here, the main tools are tensor norms in Banach space theory. In Section 5 we will discuss a physical interpretation of the probability distribution we consider on the set of quantum correlations. The conclusions of our work and future lines of research appear in Section 6.

2 Preliminary results

In this section we state some of the known, or essentially known, previous results which we will need along the paper.

The following proposition can be easily deduced from [9, Lemma 2.2].

▶ **Proposition 2.** *Let $\mathcal{G}_n$ be the gaussian measure on $\mathbb{R}^n$ and let $L \subset \mathbb{R}^n$ be a k-dimensional subspace. For a vector $g = (g_1, \cdots, g_n) \in \mathbb{R}^n$, let $\bar{g} = \frac{g}{\|g\|}$ and let $P_L(\bar{g})$ denote the orthogonal projection of $\bar{g}$ onto L. Then, for any $0 < \rho < 1$ we have*

$$\mathcal{G}_n\left((g_1, \cdots, g_n) \in \mathbb{R}^n : \quad \|P_L(\bar{g})\| \geq \frac{1}{1-\rho}\sqrt{\frac{k}{n}}\right) \leq e^{-\frac{\rho^2 k}{4}},$$

and

$$\mathcal{G}_n\left((g_1, \cdots, g_n) \in \mathbb{R}^n : \quad \|P_L(\bar{g})\| \leq (1-\rho)\sqrt{\frac{k}{n}}\right) \leq e^{-\frac{\rho^2 k}{4}}.$$

▶ Remark. As we already mentioned in the Introduction, it is completely equivalent to sample a unit vector $u \in S^{n-1}$ according to the uniform measure on the sphere μ_n to sample normalized gaussian vectors $g = \frac{1}{\|(g_1, \cdots, g_n)\|}(g_1, \cdots, g_n)$. That is, both probability distributions are exactly the same (see [6, Section 3.3] for a more complete explanation). In particular, Proposition 2 implies an analoguous statement for unitary vectors and Theorem 1 can be equivalently stated as in Theorem 6 and Theorem 9.

We say that a real random $n \times n$ matrix M is bi-orthogonally invariant if the distribution on $M_n(\mathbb{R})$ of M is equal to that of $O_1 M O_2$ for any orthogonal matrices O_1 and O_2. It is well known and easy to check that gaussian matrices are bi-orthogonally invariant.

The following result is well known, but we have not found a reference for it. It is not difficult to write a proof following the ideas of [13, Lemma 4.3.10].

▶ **Proposition 3.** *Let $A \in M_n(\mathbb{R})$ be an $n \times n$ random matrix in some probability space $(\Xi, \mathbb{P})$. If A is bi-orthogonally invariant then there exist random matrices U and V in $(\Xi, \mathbb{P})$ such that*

- **(i)** *U, V follow the Haar distribution in the orthogonal group $\mathcal{O}(n)$.*
- **(ii)** *U and V are independent.*
- **(iii)** *U and V are the matrices whose columns are respectively the left and right singular vectors associated to the ordered singular values of A.*

▶ Remark. We will use later the following easy consequence of Proposition 3: For every $n \in \mathbb{N}$ there exists a probability space Ξ with three $n \times n$ random matrices A, U, V defined on it such that A is a gaussian matrix, U, V are independent and Haar distributed in $\mathcal{O}(n)$, and for almost every $\xi \in \Xi$, $U(\xi)$ and $V(\xi)$ are the right and left singular values of $A(\xi)$ arranged in decreasing order of the singular values.

We will need the Marcenko-Pastur law, describing the distribution of the singular values of random matrices:

▶ **Theorem 4** (Marcenko-Pastur law, [14]). *Let A be an $n \times n$ random matrix whose entries a_{ij} are independent real random variables with mean 0 and variance 1. Let $C \in [0,2]$. With probability $1-o(1)$, the number of singular values λ of A that satisfy $\lambda \geq C\sqrt{n}$ is $(f(C)-o(1))n$ where*

$$f(C) = \frac{1}{2\pi}\int_{x=C^2}^{4}\sqrt{\frac{4}{x}-1}dx.$$

Here, we say that $h = h(n)$ is $o(1)$ if and only if $\lim_{n\to\infty} h(n) = 0$.

Finally, we state the version of Grothendieck's inequality most useful for our purposes (see [10, Page 172]).

▶ **Theorem 5** (Grothendieck's inequality). *There exists a universal constant K_G, such that for every natural number n and for every real matrix $(a_{i,j})_{i,j=1}^n$ we have*

$$\sup\Big\{\Big|\sum_{i,j=1}^{n} a_{i,j}\langle x_i, y_j\rangle\Big| : x_i, y_j \in B_H\Big\} \leq K_G \sup\Big\{\Big|\sum_{i,j=1}^{n} a_{i,j}s_i t_j\Big| : s_i, t_j = \pm 1\Big\},$$

where the first supremum runs over elements $x_1, \cdots, x_n, y_1, \cdots, y_n$ in the unit ball of a real Hilbert space H.

The exact value of K_G is still unknown but it is known that $1.67696... \leq K_G \leq 1.78221....$

3 A lower bound for α_0: Part (a) of Theorem 1

The precise statement for the lower bound is the following.

▶ **Theorem 6.** *Let $G = (g_{i,j})_{i,j=1}^{n,m}$ and $H = (h_{i,j})_{i,j=1}^{n,m}$ be two random matrices whose entries are independent real normalized gaussian variables satisfying $\alpha = \frac{m}{n} \in (0,1)$. For every $i,j = 1, \cdots, n$, let $g_i = (g_{i,k})_{k=1}^m$ and $h_j = (h_{j,k})_{k=1}^m$ be the row vectors of G and H respectively . Let us denote $\bar{g}_i = \frac{g_i}{\|g_i\|}$ and $\bar{h}_j = \frac{h_j}{\|h_j\|}$. Then, if $\alpha \leq \alpha_0 \approx 0.004$, the quantum correlation matrix given by $\gamma = (\langle \bar{g}_i | \bar{h}_j \rangle)_{i,j=1}^n$ is not local with probability $1-o(1)$.*

The starting point for its proof is the following result, which can be deduced from [3] and the Remark following Proposition 3. It provides an abundance of quantum nonlocal correlations when we consider the dot product of normalized truncations of orthonormal vectors.

▶ **Proposition 7.** *Let $U = (u_{i,j})_{i,j=1}^n, V = (v_{i,j})_{i,j=1}^n$ be two independent orthogonal random matrices distributed according to the Haar measure on the orthogonal group $\mathcal{O}(n)$. Let $\alpha \in (0,1)$ and $m = \alpha n$. We also denote $\delta = f^{-1}(\alpha)$, where f is the Marcenko-Pastur densitiy function as in Theorem 4. Let $\gamma_{i,j} = \langle \frac{\sqrt{n}}{\sqrt{m}}u_i, \frac{\sqrt{n}}{\sqrt{m}}v_j\rangle$ with $u_i = (u_{i,k})_{k=1}^m$ $v_j = (v_{j,k})_{k=1}^m$. Then there exists an $n \times n$ matrix $A = (a_{i,j})_{i,j=1}^n$ such that, with probability $1-o(1)$,*

$$\sum_{i,j=1}^{n} a_{i,j}\gamma_{i,j} \geq (\delta - o(1))n^{\frac{3}{2}} \quad \text{and} \quad \omega(A) \leq 1.6651\ldots n^{\frac{3}{2}}.$$

The previous proposition implies that for certain range of $\alpha = \frac{m}{n}$, the first m properly normalized columns of two Haar distributed orthogonal matrices generate a nonlocal quantum correlation with high probability. It also provides a gaussian matrix A that certifies this nonlocality. Note that the vectors $\{u_i\}_i$ (resp. $\{v_j\}_j$) are dependent of each other as they

are part of an orthogonal matrix. On the contrary, the vectors that we use to generate our correlation matrix are independent from each other.

Now, we want to approximate this columns in the appropriate norm with the corresponding columns of gaussian matrices. This is achieved with the following result from [11]. Its proof, quite technical, is based on an analysis of the Gram-Schmidt orthonormalization process and a careful use of the concentration of measure phenomenon, where Proposition 2 and similar estimates are used repeatedly.

▶ **Theorem 8** ([11, Theorem 1.1]). *Let n and m be two natural numbers such that $\alpha = \frac{m}{n} \in (0,1)$. Then, there exist matrices $Y_n = (y_{i,j})_{i,j=1}^n$ and $U_n = (u_{ij})_{i,j=1}^n$ whose $2n^2$ entries are real random variables defined on the same probability space Ξ such that*

(i) *$\{y_{i,j}; 1 \leq i,j \leq n\}$ are independent normalized random gaussian variables,*

(ii) *U_n is an orthogonal matrix distributed according to the Haar measure,*

(iii) *If we set $F_i^m(Y_n - \sqrt{n}U_n)$ the i-th row of the matrix $Y_n - \sqrt{n}U_n$ truncated to its first m entries, we have*

$$\mathbb{P}_\Xi\Big(\sup_{i=1,\cdots,n} \big\|F_i^m(Y_n - \sqrt{n}U_n)\big\| > (1+\epsilon)\theta(\alpha)\sqrt{m}\Big) \leq Kne^{C(\epsilon,\alpha)n},$$

where here K is a universal positive constant, $C(\epsilon,\alpha) > 0$ is a constant depending only on ϵ and α and

$$\theta(\alpha) = \sqrt{2 - \frac{4}{3}\frac{(1-(1-\alpha)^{3/2})}{\alpha}}.$$

Finally, Grothendieck's inequality allows us to translate this euclidean approximation between gaussian and orthonormal vectors into a big value of the correlation γ when tested against the witness A. Details can be seen in [12].

To finish this section we mention that if we consider normalized vectors u_i and v_j whose entries are independent Bernoulli variables (rather than gaussian) then we obtain local correlations with probability one. Indeed, if we consider such vectors $u_i = \frac{1}{\sqrt{m}}(\epsilon_1^i, \cdots, \epsilon_m^i)$, $v_j = \frac{1}{\sqrt{m}}(\delta_1^j, \cdots, \delta_m^j)$, we obtain that

$$(\gamma_{i,j})_{i,j=1}^n = \Big(\frac{1}{m}\sum_{k=1}^m \epsilon_k^i \delta_k^j\Big)_{i,j=1}^n.$$

However, for a fixed k, we have that $(\gamma_{i,j}^k)_{i,j=1}^n = \big(\epsilon_k^i \delta_k^j\big)_{i,j=1}^n$ is a deterministic (so local) correlation. Since $(\gamma_{i,j})_{i,j=1}^n$ is written as a convex combination of these objects, we immediately conclude that $(\gamma_{i,j})_{i,j=1}^n$ is a local correlation.

4 An upper bound for α: Part (b) of Theorem 1

The precise statement for the upper bound is the following.

▶ **Theorem 9.** *Let $G = (g_{i,j})_{i,j=1}^{n,m}$ and $H = (h_{i,j})_{i,j=1}^{n,m}$ be two random matrices whose entries are independent real normalized gaussian variables and let $\alpha = \frac{m}{n}$. For every $i,j = 1,\cdots,n$, let $g_i = (g_{i,k})_{k=1}^m$ and $h_j = (h_{j,k})_{k=1}^m$ be the row vectors of G and H respectively . Let us denote $\bar{g}_i = \frac{g_i}{\|g_i\|}$ and $\bar{h}_j = \frac{h_j}{\|h_j\|}$. Then, if $\alpha \geq 2$, the quantum correlation matrix given by $\gamma = (\langle \bar{g}_i | \bar{h}_j \rangle)_{i,j=1}^n$ is local with probability larger than $1 - 2ne^{C(\alpha)n}$. Here, $C(\alpha) \in (0,1)$ is a constant depending only on α.*

The proof of Theorem 9 relies on elements from Banach space theory: Given an $n\times n$ matrix with real entries $\Gamma = (\gamma_{i,j})_{i,j=1}^n$, we can regard this matrix as a tensor $\Gamma = \sum_{i,j=1}^n \gamma_{i,j} e_i \otimes e_j \in \mathbb{R}^n \otimes \mathbb{R}^n$. It will be convenient for us to introduce two tensor norms in this space. We define

$$\|\Gamma\|_{\ell_\infty^n \otimes_\pi \ell_\infty^n} = \inf\Big\{ \sum_{k=1}^N \|x_i\|_\infty \|y_i\|_\infty : \Gamma = \sum_{i=1}^N x_i \otimes y_i \Big\},$$

where in this definition, given a vector $z \in \mathbb{R}^n$, we denote $\|z\|_\infty = \max_{i=1,\cdots,n} |z_i|$. This norm is the projective tensor norm on $\ell_\infty^n \otimes \ell_\infty^n$ and it can be equivalently defined (see [10, Chapter 3]) as

$$\|\Gamma\|_{\ell_\infty^n \otimes_\pi \ell_\infty^n} = \inf\Big\{ \sum_{k=1}^N \lambda_k : \lambda_k \geq 0, \Gamma = \sum_{k=1}^N \lambda_k \eta_k \Big\},$$

where here η_k denotes the matrix associated to a deterministic (so local) correlation. That is, for every k we have that $\eta_k = a_k \otimes b_k$ for certain sign vectors $a_k, b_k \in \mathbb{R}^n$.

▶ Remark. It is now clear why we are interested in this norm: For a given matrix A, we trivially have that

$$\|\Gamma\|_{\ell_\infty^n \otimes_\pi \ell_\infty^n} \leq 1 \text{ if and only if } \Gamma \text{ is local (as a correlation matrix).}$$

On the other hand, we can define another tensor norm by

$$\|\Gamma\|_{\ell_\infty^n(\ell_2^n)} = \max_{i=1,\cdots,n} \|(\gamma_{i,j})_{j=1}^n\|.$$

The following result is the starting point of our proof of Theorem 9. It is a reformulation of the fact, well known in Banach space theory, that $\pi_1(id : \ell_1^n \to \ell_2^n) \leq \sqrt{2}$, where π_1 denotes the 1-summing norm (see for instance [10, Ex 11.5]).

▶ **Theorem 10.** *Given an $n \times n$ matrix with real entries $\Gamma = (\gamma_{i,j})_{i,j=1}^n$, we have that*

$$\|\Gamma\|_{\ell_\infty^n \otimes_\pi \ell_\infty^n} \leq \sqrt{2} \|\Gamma\|_{\ell_\infty^n(\ell_2^n)}.$$

To prove now Theorem 9, we use concentration of measure results to show that, with our hypothesis, $\|\Gamma\|_{\ell_\infty^n(\ell_2^n)} \leq \frac{1}{\sqrt{2}}$ with exponentially high probability. Details can be seen in [12].

5 A physical interpretation of the result

As we have said before, we consider the correlations arising from randomly uniformly distributed unit vectors as in (3). In principle, this is not a physical procedure. Nevertheless, Tsirelson proved in a constructive way that all matrices given by (3) are quantum correlations. In particular, the following result holds.

▶ **Theorem 11** ([16]). *Let $u_i = (u_{ik})_{k=1}^m, v_l = (v_{jl})_{l=1}^m \in \mathbb{R}^m$ be unit vectors. Let $\gamma = (\langle u_i, v_j \rangle)_{i,j=1}^n$. Let $X_1, \cdots, X_m : H_r \to H_r$ be m Hermitian operators, such that $X_k X_l = -X_l X_k$ if $l \neq k$ and $X_k^2 = \mathbb{1}$, where H_r is an r-dimensional Hilbert space. Then, for every $1 \leq i, j \leq n$,*

$$A_i = \sum_{k=1}^m u_{ik} X_k \text{ and } B_j = \sum_{l=1}^m v_{jl} X_l$$

are Hermitian operators of norm one and

$$\gamma_{i,j} = \langle \psi | A_i \otimes B_j | \psi \rangle,$$

where $|\psi\rangle = \frac{1}{\sqrt{r}} \sum_{s=1}^r |ss\rangle \in H_r \otimes H_r$.

Thus, given a Hilbert space H_r and operators $X_1, \cdots, X_m$ fulfilling the conditions from Theorem 11, the random correlation we are considering can be obtained physically by considering the maximally entangled state $|\psi\rangle \in H_r \otimes H_r$ and observables $\{A_i\}_i$, $\{B_j\}_j$ which are independent random linear combinations of the anticommuting observables $X_1, \cdots, X_m$.

It is known that the smallest r, so that operators $X_1, \cdots, X_m$ as above exist in H_r, is $r = 2^{[(m+1)/2]}$ (see [16]). In this case a particular choice of these operators for even m is:

$$X_{2i-1} = X \otimes^{i-1} \cdots \otimes X \otimes Y \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1} \quad \text{for every } i = 1, \cdots, m/2;$$

$$X_{2i} = X \otimes^{i-1} \cdots \otimes X \otimes Z \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1} \quad \text{for every } i = 1, \cdots, m/2,$$

where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are the Pauli matrices.

That is, with this particular choice of $X_1, \cdots, X_m$, we can physically generate quantum correlations with our probability distribution by imposing the associated probability distribution on those Pauli product measurements and measuring the maximally entangled state.

Those measurements are closely related to the measurements considered in [19], but note that in our case we increase the dimension, where in [19] the increasing parameter is the number of parties.

The main caveat to our model presented above is that it requires the physical dimension of the system to be exponential in the mathematical dimension m. We expect that there exist physical systems of much smaller dimension that give rise to quantum correlations distributed similarly to the ones we have consider, so that our techniques will apply.

6 Conclusions and future lines of research

We initiate the study of the probability of finding nonlocality among quantum probability distributions. The dual situation, studying the probability of finding games for which quantumness is an advantage over local resources, was initiated in [3].

We consider the simplest case, quantum correlations arising from bipartite dichotomic measurements. In this setting, quantum correlations can be written as the product $\gamma = (\langle u_i, v_j \rangle)_{i,j=1}^n$ of unit vectors u_i, v_j of an m-dimensional real Hilbert space H.

In this set we consider the probability distribution in the quantum correlations induced by considering the unit vectors $u_1, \ldots, u_n, v_1, \ldots, v_n$ independently uniformly distributed in the unit sphere of $\mathbb{R}^m$. This is equivalent to consider these vectors as independent normalized gaussian vectors.

We study the situation where both m and n grow to infinity with the ratio $\alpha = \frac{m}{n}$ constant.

Our main result says that in this setting two extreme situations can happen: if α is small enough (smaller than certain $\alpha_0 \approx 0.004$) then almost every such quantum correlation will be non local. But if α is big enough (greater than 2), then almost every such correlation will be local.

The tools needed to prove the first bound are random matrix theory and concentration of measure. For the second bound, the main tool are tensor norms in Banach space theory.

So far, we do not know what happens when $\alpha_0 < \alpha < 2$. In particular, we do not know if a sharp threshold behaviour between both regimes exists or not. Our techniques maybe can be refined to slightly increase the bound α_0, but they will never reach the relevant case $\alpha_0 = 1$. From the other side, our proof of part b) suggests that a more clever argument could

lead to replace 2 by K_G, but again our present approach does not seem to allow for further improvement. Along these lines, it is plausible that a relation between α and K_G describes interesting behaviors of our correlation matrices.

We provide a physical model which gives rise to our probability distribution, but it requires of an exponential (in m) physical dimension. We expect that relevant physical models of lower dimension will give rise to probability distributions close enough to ours, so that related reasonings will apply. This line of research is also open.

Until now we have only addressed the study of bipartite dichotomic quantum correlations. The study of the full probability distribution for two or more parties, or the study of N-partite dichotomic quantum correlations is totally open.

References

1 A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Device-independent security of quantum cryptography against collective attacks*, Phys. Rev. Lett. 98, 230501 (2007).

2 A. Acín, N. Gisin, and L. Masanes, *From Bell's Theorem to Secure Quantum Key Distribution*, Phys. Rev. Lett. 97, 120405 (2006).

3 A. Ambainis, A. Backurs, K. Balodis, D. Kravcenko, R. Ozols, J. Smotrovs, M. Virza, *Quantum strategies are better than classical in almost any XOR game*, Automata, Languages, and Programming Lecture Notes in Computer Science Volume 7391, 2012, 25–37.

4 A. Aspect, *Bell's inequality test: more ideal than ever*, Nature 398, 189–190 (1999).

5 A. Aspect, P. Grangier and G. Roger, *Experimental Tests of Realistic Local Theories via Bell's Theorem*, Phys. Rev. Lett. 47, 460 (1981).

6 A. Barvinok, *Measure Concentration. Math 710 Lecture Notes*, Department of Mathematics, University of Michigan (2005).

7 J. S. Bell, *On the einstein-podolsky-rosen paradox*, Physics 1, 195–200 (1964).

8 H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, *Nonlocality and communication complexity*, Rev. Mod. Phys. 82, 665 (2010).

9 S. Dasgupta, A. Gupta, *An elementary proof of a theorem of Johnson and Lindenstrauss*, Random Struct. Alg. 22(1), 60–65 (2003).

10 A. Defant and K. Floret, *Tensor Norms and Operator Ideals*, North-Holland, (1993).

11 C. E. González-Guillén, C. Palazuelos, I. Villanueva, *Euclidean distance between Haar orthogonal and gaussian matrices*. arXiv:1412.3743.

12 C. E. González-Guillén, C. H. Jimenez, C. Palazuelos, I. Villanueva, *Sampling quantum nonlocal correlations with high probability*. arXiv:1412.4010.

13 F. Hiai and D. Petz, *The semicircle law, free random variables and entropy*, American Mathematical Society Providence, (2000).

14 V. A. Marcenko, L. A. Pastur, *Distribution of eigenvalues for some sets of random matrices*, Math. USSR Sbornik, 1:457–483, (1967).

15 S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning and C. Monroe, *Random numbers certified by Bell's theorem*, Nature (London) 464, 1021 (2010).

16 B. S. Tsirelson, *Some results and problems on quantum Bell-type inequalities*, Hadronic J. Supp. 8(4), 329–345 (1993).

17 U. Vazirani, T. Vidick, *Fully device-independent quantum key distribution*, available in arXiv:1210.1810 (2012).

18 U. Vazirani, T. Vidick, *Certifiable quantum dice – Or, exponential randomness expansion*, Phil. Trans. R. Soc. A, 370, 3432–3448 (2012).

19 J. J. Wallman, Y.-C. Liang, S. D. Bartlett, *Generating nonclassical correlations without fully aligning measurements*, Phys. Rev. A 83, 022110 (2011).